ABSTRACT

thesis of **Ussatova O.A.**
on the topic: « Development and research of an authentication algorithm for users of information and communication systems»
submitted for the degree of Doctor of Philosophy (PhD) in the specialty 6D100200 – «Information Security Systems»

Since the independence of the Republic of Kazakhstan, its first president, Nursultan Abishevich Nazarbayev, has repeatedly focused on the need to protect the interests of citizens in the Republic of Kazakhstan. Thus, in the Address of the President of the country to the people of Kazakhstan dated October 10, 1997, "Kazakhstan is 2030. Prosperity, Security, and Improving the Welfare of All Kazakhstanis," state security is established as a long-term priority, where information security is one of the important directions.

The complex mechanism of information security processes in our Republic covers organizational, social, technical and programmatic approaches that are able to exercise the constitutional rights and freedom of a person, a citizen in the field of obtaining information, using it to protect the constitutional system, sovereignty and territorial integrity of the Republic of Kazakhstan, financial, and also social sustainability, the formation of a profitable international partnership in the field of informative security.

The Law "On National Security of the Republic of Kazakhstan" adopted on January 6, 2012 contains the necessary articles, which give clear definitions from the position of the state, affecting the information security of the country as a whole and citizens in particular.

At the legislative level in the Republic of Kazakhstan, a national concept of ensuring information security, electronic document management, automated information systems, resources, ICT, and also important objects is being formed and fixed.

When constructing and operating telecommunication communication networks, it is necessary to take into account the requirements of the Republic of Kazakhstan on compliance with national security in the field of communications. This is evidenced by the latest amendment to the article "On the powers of state bodies of the Republic of Kazakhstan" dated December 27, 2017.

On May 21, 2013, the Law of the Republic of Kazakhstan (RK) No. 94-V "On personal data and their protection" (with amendments and additions as of December 28, 2017) was adopted, it regulates relations related to the collection and processing, as well as the protection of personal data. Important are the Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V "On Informatization" (as amended as of 01.01.2020) and the Law of the Republic of Kazakhstan dated January 7, 2003 No. 370-II "On electronic document and electronic digital signature "(as amended as of November 25, 2019).

The development of information and telecommunication technologies allows using new opportunities on the Internet. There was an opportunity to make remote

purchases of goods from anywhere in the country, to monitor the status and execution of work, without being present at the places of their conduct. Currently, it is possible to issue almost any certificate without leaving your home, thanks to an electronic digital signature and the information portal of public services.

In the Republic of Kazakhstan on December 12, 2017, Government Decision No. 827 approved the state program "Digital Kazakhstan". In this program, the main aspect is the development of the country's economy and the increase in the life of the population, based on improving and accelerating the development of information and communication technologies and also creating a digital economy. The main attention is paid to ensuring information security in the field of information and communication technologies and the consolidation of cyber security of automated information systems in our country.

With the development of technological progress and the general level of informatization, new threats also appear. Cybercrime allows cybercriminals to commit unlawful and illegal actions, being thousands of kilometers from the target of their attack. In the Address to the people of Kazakhstan “Third Modernization of Kazakhstan: Global Competitiveness”, the President of the Republic of Kazakhstan noted that the fight against cybercrime is becoming increasingly relevant. In this regard, the Concept of Cyber security (“Cyber shield of Kazakhstan”) was developed and approved by Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407, it defines the main directions for implementing state policy in the field of protection of electronic information resources, information systems and telecommunication networks, ensuring safe use of information and communication technologies.

Information technology has become an integral part of our life, in connection with this, many processes of human life are automated. Most of the information is stored in information systems, which must be protected. In attacks on information systems, attackers use both errors in writing and administering programs, and methods of social psychology to obtain the desired information. Resource developers who are supposed to work with user data are required to protect this data and prevent the possibility of leakage. One of the main problems of the Republic of Kazakhstan is the weak development of the domestic industry of information security, in particular in the development of cryptography tools. In Kazakhstan, current cryptographic algorithms and standards are used in existing electronic data protection systems. Studies regarding data security are directly combined with state secrets and the use of ready-made foreign solutions is very risky, in this regard, it is necessary to create your own resources for information security.

In IICT SC MES RK research work is underway on cryptographic information protection and access control. The employees of the Information Security Laboratory are engaged in this research (the head of the laboratory, doctor of technical sciences, professor R. Biyashev, academician of the National Academy of Sciences of the Republic of Kazakhstan Kalimoldaev M.N., doctor of technical sciences, assistant professor N. Nysanbaeva ., ANS, Ph.D. Kapalova N.A., PhD Begimbaeva E.E., Researchers O.A. Rog, D.S. Dyusembaev, K.E. Algazy, A.V. Varennikov and others).

One of the main means of protecting information systems from outside interference is identification and authentication, since information protection mechanisms are designed to work with named subjects and objects. Authentication and user authentication are interdependent actions of recognition and authentication.

The main purpose of user authentication of an information system is to reduce security threats, namely violation of confidentiality and integrity of information. Unauthorized access is one of the most common types of violations that poses a direct threat to the health of the system.

Authentication is used to access social networks, email, online shopping, online banking, payment systems, etc. User authentication is classified into the following types:

– password-based authentication: it is performed using one-time and reusable passwords. The reusable password is set by the user, and the system stores it in the database. It is the same for each session. These include PIN codes, words, numbers, pattern keys. One-time passwords for each session are different;

– combined authentication, which occurs using several methods, for example, password and cryptographic certificates. It requires a special device for reading information;

– biometric authentication: it prevents the leakage or theft of personal information. The test is based on the physiological characteristics of the user, for example, fingerprint, retina, face recognition and voice timbre.

Currently, the use of password authentication is affordable and widespread due to its ease of use. This security method leads to an increase in the strength of the information security concept. One of the effective methods of protecting information is two-factor authentication for entering the system. It involves double data protection by linking the account to the protection system. After binding, the user will need to interact with this system to verify the data.

The problems of information security, access control and authentication based on the second factor were dealt with by foreign scientists Edna Elizabeth, S. Niveta, Faseh Sadat Babamir, Murvet Kirchi, Yui, Jingshahe, Nafei Zhu, Fanbo Tsai, Mohammed Salman Patan and others. It is also important to protect information stored in databases and hardware and software for processing and transmitting information. A significant contribution to the development of this direction was also made by foreign scientists R. Meshcheryakov, A. Yu. Iskhakov, Poltavtseva M.A. and others.

As it was said before, the topic of this thesis on the development and research of an authentication algorithm for users of information and communication systems based on the second factor is relevant. In this dissertation, a one-time password is the second factor.

The relevance of the study is the need:

– implementation of the tasks set in the State Program of the Government of the Republic of Kazakhstan and the Concept of Cyber security (“Cyber shield of Kazakhstan”) aimed at developing a state policy in the field of protection of electronic

information resources, telecommunication systems and networks, ensuring the safe use of information and communication technologies;

– development of domestic Kazakhstan information security systems;

– applying a two-factor password authentication policy to increase the reliability of information security systems.

The purpose of the dissertation research: the development, research, and implementation of a two-factor authentication algorithm to ensure the protection of information in information and communication systems.

Research objectives that implement the purpose of the dissertation research:

1. Review and analysis of existing information about security systems in information and communication systems and multi-factor authentication algorithms.
2. Development of an authentication algorithm for users of information and communication systems using a one-time password.
3. Creating an information system to ensure the integrity and protection of information in information and communication systems.

The object of study: a system of protecting information from unauthorized access during user authentication based on the second factor.

The subject of the research is the processes of information interaction between users of information and communication systems and their authentication using a one-time digital password.

The scientific novelty of the studies and the results obtained in the work:

- an algorithm of two-factor user authentication was developed based on the generation of trigonometric functions by complicating the scaling of functions when calculating a one-time password; scaling is performed by the matrix representation of trigonometric function variants and using hash functions to calculate the coordinates and parameters of the trigonometric function generated by the current time, secret line, login and password of the first authentication code;
- a model of the process of two-factor user authentication based on the second factor was developed, which differs from the known ones in the facts that it is open and can generate sets of functions for obtaining a second authentication code for each individual system;
- a scheme of the information system for the software implementation of two-factor authentication using a mobile device for its implementation and use in a closed network is proposed.

Personal contribution of the researcher. An algorithm for user authentication of the information system based on the second factor is developed. Numerical studies and experimental evaluation of the proposed models and algorithms are carried out. The client-server authentication system architecture has been developed and software implementation of the proposed user authentication system has been implemented when generating a one-time password using an authenticator computer program and a mobile phone.

The connection of the topic with the plans of research programs. The presented results were obtained during the implementation of the following projects of the Institute of Science and Technology of the Ministry of Education and Science

of the Republic of Kazakhstan (funding source: Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan):

– program-targeted financing (PCF) of the Ministry of Education and Science of the Republic of Kazakhstan "Development of software and hardware for cryptographic protection of information during its transmission and storage in info-communication systems and general-purpose networks" in 2018-2019;

– grant financing (GF) of the Ministry of Education and Science of the Republic of Kazakhstan "Development of the Kazakh segment of secure cross-border information interaction" in 2020.

Publications. The main results of the research on the topic of the dissertation are presented in 15 publications, of which 5 - in scientific journals recommended by the Ministry of Education and Science of the Republic of Kazakhstan, 2 - in international scientific journals included in the Scopus and Web of Science database, 8 - in materials of international scientific and practical conferences.

The structure and scope of the dissertation. The total amount of work is 123 pages. The dissertation consists of an introduction, 3 sections, a conclusion, a list of sources used, where 104 items, 4 appendices, includes 37 figures and 5 tables.

The introduction provides a rationale for the relevance of the chosen topic of the dissertation research. The goal, object, subject, and objectives of the study are formulated. The results of the research are described, their scientific novelty and practical significance are shown. The data on the approbation of the results of the thesis are presented.

The first section is devoted to the study of well-known methods and means of protecting information systems based on two-factor authentication. The principles of building information security in the database during user authentication are described.

The classification of the common methods of two-factor authentication used in information systems is presented, the disadvantages and advantages of these methods are considered.

Algorithms and authentication protocols using a one-time code are considered. HOTP (HMAC - Based One - Time Password Algorithm) - a secure authentication algorithm using a one-time code based on SHA-1 and TOTP (Time - based One - Time Password Algorithm) - a one-time password creation algorithm for secure authentication, which is the foundation for the development of one-time secure authentication passwords. The analysis of information security systems and their characteristics based on two-factor authentication is carried out.

The statistical data of companies specializing in the field of information security are described. An analysis of cyberattacks was carried out and some companies providing services to protect information stored in databases were examined. The problems that arise when using ready-made solutions of authenticators are described. The statistical data of companies specializing in the field of information security. An analysis of cyberattacks was carried out and some companies providing services to protect information stored in databases were examined. The problems that arise when using ready-made solutions of authenticators are described.

The second section presents the results obtained during the development of the security model of the information system during user identification based on two-factor authentication. Authentication methods using a one-time password are considered. An algorithm for generating a one-time password using an authenticator program and a mobile phone is developed and described, which is based on a one-time-key generation model for user authentication based on the second factor. The developed model is based on a combination of two factors: permanent and temporary passwords.

The SHA256 hash function is described, which is used as an input parameter to generate a set of functions and calculate a one-time password. To generate the SHA256 hash function, such data as the user login and password, the current time/date, and the secret line are taken into account. The created generators of random secret words and trigonometric functions for generating a one-time password for two-factor authentication are considered.

The third section presents the results of the software implementation of the previous two-factor authentication algorithm. An information system consisting of 3 interacting modules is developed: user, mobile application, and server part. The structures of each of these modules are considered.

The Base64 algorithm and its usage scheme for protecting information stored in a database with the given program code in the JavaScript implementation language are described. The standard TLS (Transport Layer Security) and SSL (Secure Socket Layer) protocols for protecting website traffic and file sharing over the network are considered.

The work of the MongoDB DBMS, in which data is stored and processed, is described. The object-oriented approach used in the implementation of the algorithm is described. The structure of the application is described in stages. The computer implementation of the information security information system during user authentication based on a one-time-key was carried out and the correctness of the proposed algorithm was investigated. In conclusion, the main results and findings of the thesis are stated.

The results of the study are included in the reports of the above-mentioned PCF projects for 2018-2019 and the Global Fund for 2020, carried out at the Information Security Laboratory of the Institute of Information Technologies and Computer Science of the Ministry of Education and Science of the Republic of Kazakhstan.

Reliability level and testing results. The validity and reliability of the study correspond to the substantiated responsibilities of the task, the analysis of the criteria and the state of research in this area, a large number of experiments, and their successful implementation in practice. The results of the dissertation were discussed and reported at the following scientific and methodological conferences:

1. International scientific-practical conference “Innovative technologies in transport: education, science, practice” in the framework of the Address of the President of the Republic of Kazakhstan N. Nazarbayev “New development opportunities in the conditions of the fourth industrial revolution” (Kaz ATK, Kazakhstan, Almaty, 2018);

2. Scientific conference "Modern Problems of Informatics and Computing Technologies" (IICT SC MES RK, Kazakhstan, Almaty, 2018);

3. International scientific conference “Informatics and Applied Mathematics” (IITT KN MON RK, Kazakhstan, Almaty, 2018);

4. The international scientific and methodological conference dedicated to the 90th anniversary of the Kazakh National Pedagogical University named after Abai (Kaz NPU, Kazakhstan, Almaty, 2018);

5. International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019) (Guilin, China, 2019);

6. Scientific conference "Modern Problems of Informatics and Computing Technologies" (IITT KN MON RK, Kazakhstan, Almaty, 2019);

7. International scientific-practical conference "Informatics and Applied Mathematics" (IITT KN MON RK, Kazakhstan, Almaty, 2019);

8. International scientific-practical conference "Actual problems of information security in Kazakhstan" (IITT KN MON RK, Kazakhstan, Almaty, 2020).

On the topic of the dissertation, 15 articles were published and 2 copyright certificates were obtained:

1 Нысанбаева С.Е., Усатова О. А. «Способы обеспечения безопасности информации в базах данных»//Вестник КазНИТУ им. Сатпаева. – Алматы, 2018. – № 2. – С. 66–70.

2 Нысанбаева С.Е., Усатова О.А. «Возможное применение больших данных в системе образования»// Матер. междунар. науч. практ. конф. «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции» – Алматы, 2018. – С. 95–99.

3 Нысанбаева С.Е., Усатова О.А. «Криптографическая защита в автоматизированных системах»// Науч. конф. «Современные проблемы информатики и вычислительной технологий». – Алматы, 2018. – С. 220–223.

4 Нысанбаева С.Е., Усатова О.А. «Двухфакторная аутентификация в автоматизированной системе управления»// III Междунар. науч. конф. «Информатика и прикладная математика». – Алматы, 2018. – С. 239–242.

5 Усатова О.А., Науменко В.В. «Статистические исследования инфраструктурной платформы с использованием систем защиты данных»// VIII междунар. науч.-метод. конф. посвященной 90-летнему юбилею Казахского национального педагогического университета имени Абая. – Алматы, 2018. – С. 113–116.

6 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Development of an authentication model based on the second factor in an automated control system»// Вестник КБТУ. – Алматы, 2019. –Т.16. – С.115–118.

7 S. Nyssanbayeva, W. Wojcik, O. Ussatova. «Algorithm for generating temporary password based on the two–factor authentication model»// Przegląd Elektrotechniczny. – Polan, 2019. –№ 5. – P. 101–106.

8 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Two-factor authentication algorithm implementation with additional security parameter based on mobile

application »// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). –Guilin, China, 2019. – Vol. 89. – P. 84–86.

9 O. Ussatova, S. Nyssanbayeva, W. Wojcik. « Software implementation of two-factor authentication to ensure security when accessing an information system» // Вестник КазНУ им.аль-Фараби. –Алматы,2019. – С.87–95.

10 Olga Ussatova, Saule Nyssanbayeva. «Generators of one-time two-factor authentication passwords»// Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. – Poland, 2019. № 2. – P. 60–64.

11 Усатова О.А., Нысанбаева С.Е. «Обеспечение защиты информационной системы с помощью двухфакторной аутентификации»// науч. конф. «Современные проблемы информатики и вычислительных технологий» – Алматы, 2019. –С. 337–343.

12 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule. «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311 916. 2020.1724597. –P. 1–13.

13 Бегимбаева Е.Е., Усатова О.А., Бияшев Р.Г., Нысанбаева С.Е., Вуйцик В., «Разработка модулей для защиты информации в автоматизированной системе с применением разграничения доступа»// IV междунар. науч.– практ. конф. «Информатика и прикладная математика», посвященная 70–летнему юбилею профессоров Биярова Т.Н., Вальдемара Вуйцика и 60–летию профессора Амиргалиева Е.Н. – Алматы, 2019. – С. 595–602.

14 Усатова О.А., Нысанбаева С.Е. «Исследование и разработка модели защиты базы данных информационной системы»// Вестник КазНУ им.аль–Фараби, Алматы, 2019. – № 4 (104), – С.95–106.

15 Усатова О.А. «Клиент-серверная система защиты информации на основе двухфакторной аутентификации»// междунар. науч.– практ. конф. «Актуальные проблемы информационной безопасности в Казахстане». – Алматы, 2020. – С. 243–248.

16 Сертификат регистрации авторского права на алгоритм «Двухфакторная аутентификация в автоматизированной системе управления» №712144534 от 2018.10.01, компании «WORKS COPYRIGHT», это цифровая сертификация, юридически признанная во всем мире для регистрации авторских прав авторов, New York – NY–USA.

17 Авторское свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом РК, № 4330 от 28 июня 2019г., «Система аутентификации с использованием второго фактора для контроля доступа к данным – Security Code of the 2FA».